
Contents

1	Open-source intelligence evolution and basics	1
1.1	<i>Introduction</i>	1
1.2	<i>Intelligence lifecycle</i>	2
1.2.1	<i>Stage 1: Planning and direction</i>	3
1.2.2	<i>Stage 2: Collection</i>	4
1.2.3	<i>Stage 3: Processing and exploitation</i>	5
1.2.4	<i>Stage 4: Analysis and production</i>	6
1.2.5	<i>Stage 5: Dissemination</i>	7
1.3	<i>Role of OSINT</i>	8
1.4	<i>Open-source v/s classified information</i>	13
1.5	<i>OSINT principles</i>	14
1.5.1	<i>Transparency: unveiling the truth</i>	14
1.5.2	<i>Legality: operating within the boundaries of the law</i>	15
1.5.3	<i>Relevance: focusing on what matters</i>	16
1.5.4	<i>Ethical landscape of OSINT</i>	17
1.5.5	<i>Pursuing truth and precision</i>	18
1.5.6	<i>Upholding integrity & accountability</i>	18
1.6	<i>Historical evolution of OSINT</i>	19
1.7	<i>Modern OSINT</i>	23
1.8	<i>OSINT data sources</i>	25
1.9	<i>Critical thinking and OSINT process</i>	28
1.10	<i>Conclusion</i>	32
	<i>References</i>	33
2	Online privacy and secure browsing techniques	34
2.1	<i>Introduction</i>	34
2.2	<i>Understanding the threat landscape</i>	35
2.2.1	<i>Rise of surveillance capitalism</i>	35
2.2.2	<i>Encryption and anonymization</i>	36

2.3	<i>Privacy-focused techniques</i>	38
2.3.1	<i>Virtual private networks or VPNs</i>	38
2.3.2	<i>The Onion Router (Tor) browser</i>	40
2.3.3	<i>Privacy-focused search engines</i>	42
2.3.4	<i>Privacy extensions</i>	45
2.3.5	<i>Cookie managers</i>	50
2.3.6	<i>Password managers</i>	51
2.3.7	<i>Script blockers</i>	52
2.3.8	<i>Privacy shields</i>	53
2.4	<i>Conclusion</i>	54
	<i>References</i>	54
3	Building OSINT skills and workflow process	56
3.1	<i>Introduction</i>	56
3.2	<i>Psychology</i>	56
3.3	<i>Communications & people skills</i>	57
3.4	<i>Numerical analysis</i>	58
3.5	<i>Research</i>	59
3.6	<i>Ethics</i>	60
3.7	<i>Legal skills and knowledge</i>	60
3.8	<i>Problem-solving</i>	61
3.9	<i>Technical skills</i>	62
3.10	<i>Patience</i>	63
3.11	<i>OSINT workflow process</i>	64
3.12	<i>Conclusion</i>	65
	<i>References</i>	66
4	Search underground internet	67
4.1	<i>Introducing the dark web</i>	67
4.2	<i>Ethical considerations</i>	68
4.3	<i>Law enforcement and the dark web</i>	69
4.4	<i>Dark web sites</i>	70
4.4.1	<i>The Hidden Wiki</i>	70
4.4.2	<i>Silk Road</i>	72
4.4.3	<i>AlphaBay</i>	75
4.5	<i>Perform dark web search</i>	76
4.6	<i>Conclusion</i>	84
	<i>References</i>	84

5 OSINT search engine techniques 85

- 5.1 OSINT search 85
- 5.2 Maltego 86
- 5.3 OSINT framework 94
- 5.4 Shodan 94
 - 5.4.1 Hands-on: explore critical infrastructure 96
 - 5.4.2 Hands-on: explore enterprise systems 102
 - 5.4.3 Hands-on: explore home devices 105
- 5.5 Google Dorking 114
 - 5.5.1 Uncover sensitive documents 114
 - 5.5.2 Search location-specific targets 115
- 5.6 OSINT email identification 117
- 5.7 Network security assessment Dorks 118
- 5.8 Conclusion 126
- References 126

6 Email address intelligence 128

- 6.1 Introduction 128
- 6.2 Analyzing use cases 130
 - 6.2.1 Use case #1: email address analysis of valid ID 130
 - 6.2.2 Use case #2: email address analysis of potential spammers 132
 - 6.2.3 Use case #3: email address analysis of spammers 132
 - 6.2.4 Use case #4: TheHarvester 133
 - 6.2.5 Use case #5: Holehe 138
 - 6.2.6 Use case #6: gather Gmail account information 138
- 6.3 Find email address from Facebook ID 145
- 6.4 Find email address using Chrome extension 148
- 6.5 Search business email address 153
- 6.6 Conclusion 161
- References 162

7 Imagery intelligence 163

- 7.1 Introduction 163
- 7.2 Image intel use cases 164
 - 7.2.1 Use case #1 164
 - 7.2.2 Use case #2 164
 - 7.2.3 Use case #3 173

7.2.4	<i>Use case #4</i>	176
7.2.5	<i>Use case #5</i>	178
7.2.6	<i>Use case #6</i>	180
7.2.7	<i>Use case #7</i>	185
7.2.8	<i>Use case #8</i>	185
7.2.9	<i>Use case #9</i>	190
7.3	<i>Fighting child exploitation online</i>	191
7.4	<i>Conclusion</i>	192
	<i>References</i>	192

8 Tracking satellites and aircrafts 193

8.1	<i>Introduction</i>	193
8.2	<i>GEOINT challenges</i>	194
8.3	<i>Metadata challenges</i>	195
8.4	<i>Satellite OSINT</i>	198
8.4.1	<i>Use case #1</i>	199
8.4.2	<i>Use case #2</i>	201
8.4.3	<i>Use case #3</i>	206
8.5	<i>Aircraft OSINT</i>	207
8.5.1	<i>Use case #1</i>	209
8.5.2	<i>Use case #2</i>	210
8.5.3	<i>Use case #3</i>	211
8.5.4	<i>Use case #4</i>	213
8.5.5	<i>Use case #5</i>	214
8.5.6	<i>Use case #6</i>	216
8.6	<i>Conclusion</i>	218
	<i>References</i>	220

9 Tracking maritime and land-based transportation 222

9.1	<i>Maritime OSINT</i>	222
9.1.1	<i>Geolocation analysis</i>	222
9.1.2	<i>Analyzing vessel red flags</i>	223
9.1.3	<i>Monitoring maritime social media</i>	223
9.1.4	<i>Investigating illegal fishing</i>	223
9.1.5	<i>Detecting maritime piracy</i>	224
9.1.6	<i>Monitoring environmental impacts</i>	224
9.2	<i>Use cases</i>	224
9.2.1	<i>Use case #1</i>	224
9.2.2	<i>Use case #2</i>	227
9.2.3	<i>Use case #3</i>	229

9.2.4	<i>Use case #4</i>	230
9.2.5	<i>Use case #5</i>	234
9.2.6	<i>Use case #6</i>	236
9.3	<i>Land-based transportation OSINT</i>	237
9.3.1	<i>Tracking vehicle movements</i>	237
9.3.2	<i>Analyzing vehicle ownership and affiliations</i>	239
9.3.3	<i>Monitoring social media for transportation intelligence</i>	239
9.3.4	<i>Investigating infrastructure vulnerabilities</i>	240
9.3.5	<i>Detecting smuggling and trafficking</i>	240
9.3.6	<i>Monitoring transportation security</i>	240
9.4	<i>Conclusion</i>	241
	<i>References</i>	241
10	Conclusion	243
10.1	<i>Open-source intelligence evolution and basics</i>	243
10.2	<i>Online privacy and secure browsing techniques</i>	244
10.3	<i>Building OSINT skills and workflow process</i>	245
10.4	<i>Search underground internet</i>	247
10.5	<i>OSINT search techniques</i>	248
10.6	<i>Email address intelligence</i>	249
10.7	<i>Imagery intelligence</i>	250
10.8	<i>Tracking satellites and aircrafts</i>	251
10.9	<i>Conclusion</i>	252